UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/858,336	05/15/2001	Philip R. Patterson	P0366	1102

23735 7590 08/25/2003

DIGIMARC CORPORATION
19801 SW 72ND AVENUE
SUITE 100
TUALATIN, OR 97062

EXAMINER
WANG, JIN CHENG

ART UNIT	PAPER NUMBER
2672	7

DATE MAILED: 08/25/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/858,336	PATTERSON ET AL.	
	Examiner	Art Unit	
	Jin-Cheng Wang	2672	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____ .

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 9-29 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 9-29 is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Response to Amendment

1. The amendment filed on 8/01/2003 has been entered. Claims 1-8 have been cancelled. Claims 23 and 28 have been amended.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 9-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Levy et al. U.S. Pat. No. 6,505,160 (hereinafter Levy).

4. Claim 9:

Levy teaches a method for managing images, the images including a first image comprising a first identifier steganographically embedded in the first image in the form of a digital watermark (column 2, lines 22-37), said method comprising the steps of:

(a) Retrieving the first image from a database (e.g., column 13, lines 29-67; column 14, lines 1-35);

(b) Altering the first image to create a second image (e.g., column 4, lines 10-13; column 8, lines 8-19; column 8, lines 65-67; column 9, lines 1-6; column 10, lines 4-17; column 15, lines 55-62);

(c) Steganographically embedding a second identifier in the second image in the form of a digital watermark (e.g., column 15, lines 16-62);

(d) Associating the second image in the database with the first identifier (e.g., column 15, lines 55-62; column 13, lines 29-67; column 14, lines 1-35).

Claim 10:

The claim 10 encompasses the same scope of invention as that of claim 9 except additional claimed limitation of removing the first identifier from the second image. However, Levy further discloses the claimed limitation of removing the first identifier from the second image (column 15, lines 24-34).

Claim 11:

The claim 11 encompasses the same scope of invention as that of claim 9 except additional claimed limitation of altering the first identifier in the second image. However, Levy further discloses the claimed limitation of altering the first identifier in the second image (column 15, lines 24-34).

Claim 12:

The claim 12 encompasses the same scope of invention as that of claim 9 except additional claimed limitation of storing information related to the first image in the database. However, Levy further discloses the claimed limitation of storing information related to the first image in the database (column 7, lines 13-20).

Claim 13:

The claim 13 encompasses the same scope of invention as that of claim 12 except additional claimed limitation of the related information comprising at least one of metadata, location, date, permission level, security access levels, analyst comments, notes, files, and past usage information. However, Levy further discloses the claimed limitation of the related information comprising at least one of metadata, location, date, permission level, security access levels, analyst comments, notes, files, and past usage information (column 6, lines 5-28, column 14, lines 30-33).

Claim 14:

The claim 14 encompasses the same scope of invention as that of claim 13 except additional claimed limitation of the database comprising a plurality of databases.

However, Levy further discloses the claimed limitation of the database comprising a plurality of databases (column 14, lines 1-9).

5. Claims 15-29 are rejected under 35 U.S.C. 102(e) as being anticipated by Glass et al. U.S. Pat. No. 6,332,193 (hereinafter Glass).

6. Claim 15:

Glass teaches a method to monitor images in a system, the system comprising at least a first user terminal (e.g., a client computer or a bank computer with a secured resource; see figures 6-7) to communicate with a second user terminal (e.g, a client computer or a banking system with a secured resource) and with a database (e.g., a central database, column 9, lines 8-25, column 10, lines 3-5), the images comprising at least a first image digitally watermarked to

include a first identifier (e.g, column 7, lines 3-33; column 9, lines 5-60), said method comprising the steps of:

Determining a security level (digital signature embedded into the image) associated with the first image (column 9, lines 8-60);

Comparing (column 9, lines 40-50) the first image security level (digital signature) with a user security level (i.e., the server's copy of the secret key; see column 6, lines 50-56; by the image authentication module 15, column 9, lines 5-60); and

Allowing access (by the client computer or the banking system with a secured resource; figures 6-7) to the first image (e.g., the original secured image data originally sent by the client) based on a result of said comparison step (column 9, lines 8-60).

Claim 16:

The claim 16 encompasses the same scope of invention as that of claim 15 except additional claimed limitation of recording a transmission in the database of the first image from the first user terminal to the second user terminal. However, Glass further discloses the claimed limitation of recording a transmission in the database of the first image from the first user terminal to the second user terminal (e.g., column 9, lines 51-67; column 10, lines 1-10).

Claim 17:

The claim 17 encompasses the same scope of invention as that of claim 15 except additional claimed limitation of decoding the digital watermark to determine the first identifier and interrogating the database with the first identifier to retrieve the security level.

However, Glass further discloses the claimed limitation of decoding the digital watermark to determine the first identifier (e.g., the image authentication module 15, column 9, lines 44-60, column 7, lines 12-30) and interrogating the database with the first identifier to retrieve the security level (e.g., column 9, lines 51-67; column 10, lines 1-10).

Claim 18:

The claim 18 encompasses the same scope of invention as that of claim 15 except additional claimed limitation that the first image's digital watermark includes security level data, and wherein the determining step comprises the step of decoding the digital watermark to determine the security level.

However, Glass further discloses the claimed limitation that the first image's digital watermark includes security level data (digital signature comprises user's signature information, a token and camera's secret key, column 9, lines 29-31), and wherein the determining step comprises the step of decoding the digital watermark to determine the security level (e.g., column 9, lines 5-67; column 10, lines 1-10, column 7, lines 5-30).

Claim 19:

The claim 19 encompasses the same scope of invention as that of claim 15 except additional claimed limitation that the user security level comprises at least one of a security level for a user and a security level for a user terminal.

However, Glass further discloses the claimed limitation that the user security level comprises at least one of a security level for a user (e.g., a digital signature, column 8, lines 55-62) and a security level for a user terminal (the secret key embedded in each camera, column 8, lines 63-67, column 54-60).

Claim 20:

The claim 20 encompasses the same scope of invention as that of claim 15 except additional claimed limitation that when the result is a match between the first image security level and the user security level access is allowed.

However, Glass further discloses the claimed limitation that when the result is a match between the first image security level and the user security level access is allowed (e.g., column 6, lines 50-56; authentication, column 9, lines 44-60).

Claim 21:

The claim 21 encompasses the same scope of invention as that of claim 15 except additional claimed limitation that the match indicates that the user security level is equal to or greater than the first image security level.

However, Glass further discloses the claimed limitation that the match indicates that the user security level is equal to or greater than the first image security level (e.g., column 9, lines 44-60).

Claim 22:

The claim 22 encompasses the same scope of invention as that of claim 15 except additional claimed limitation of recording access to the image.

However, Glass further discloses the claimed limitation of recording access to the image (e.g., column 9, lines 54-67; column 10, lines 1-10).

7. Claim 23:

Glass teaches a system comprising:

A first user terminal (a client computer or a banking computer; see figures 6-7);

A second user terminal (e.g., a client computer or a banking computer having the protected resource, or a server system associated with another computer system that performs online banking transactions, column 8, lines 25-34);

A database (e.g., a central database, column 10, lines 1-9, column 8, lines 22-52), wherein the first user terminal (e.g., a client computer or a banking computer having the protected resource, or a server system associated with another computer system that performs online banking transactions, see figures 6-7) and the second user terminal (e.g., a client computer or a banking computer having the protected resource, or a server system associated with another computer system that performs online banking transactions, see figures 6-7; column 8, lines 25-34) are in communication (over a network of figures 6-7), and the first user terminal and the second user terminal are each in communication with the database (i.e., central database, column 10, lines 1-9); and

A gatekeeper (the authentication server, column 8, lines 55-67) to regulate the flow of at least a first image between the first user terminal and the second user terminal, wherein the first image comprises at least a first digital watermark (e.g., column 7, lines 3-33; column 9, lines 5-67; column 10, lines 1-10) including a first identifier, said gatekeeper to determine a security level associated with the first image (column 9, lines 26-60), compare the first image security level with a user security level (e.g., compute a signature of the original data and check it against the signature sent with the data to see if the signature match, column 6, lines 50-56, column 9, lines 26-60), and to allow access by the second user terminal to the first image based on a result of the comparison (column 6, lines 50-56; column 9, lines 5-67; column 10, lines 1-10).

Claim 24:

The claim 24 encompasses the same scope of invention as that of claim 23 except additional claimed limitation that the gatekeeper records in the database a transmission of the first image from the first user terminal to the second user terminal. However, Glass further discloses the claimed limitation that the gatekeeper records in the database a transmission of the first image from the first user terminal to the second user terminal (column 9, lines 55-60).

Claim 25:

The claim 25 encompasses the same scope of invention as that of claim 23 except additional claimed limitation that the gatekeeper comprises software to decode the digital watermark to determine the first identifier, and to interrogate the database with the first identifier to retrieve the security level.

However, Glass further discloses the claimed limitation that the gatekeeper comprises software (the authentication module 15) to decode the digital watermark to determine the first identifier (column 9, lines 26-60), and to interrogate the database with the first identifier to retrieve the security level (column 10, lines 1-9).

Claim 26:

The claim 26 encompasses the same scope of invention as that of claim 23 except additional claimed limitation that the first image digital watermark includes security level data, and wherein the gatekeeper comprises software code to decode the digital watermark to determine the security level data.

However, Glass further discloses the claimed limitation that the first image digital watermark includes security level data (the signature information, column 7, lines 3-33), and wherein the gatekeeper comprises software code to decode the digital watermark to determine the security level data (column 9, lines 26-60).

Claim 27:

The claim 27 encompasses the same scope of invention as that of claim 23 except additional claimed limitation that the user security level comprises at least one of a security level for a user and a security level for a user terminal.

However, Glass further discloses the claimed limitation that the user security level comprises at least one of a security level for a user (biometric identification, column 8, lines 55-62) and a security level for a user terminal (the secret key embedded in each camera, column 8, lines 63-67, column 54-60).

8. Claim 28:

Glass teaches a module (authentication module 15) for use in a network comprising at least a first terminal in communication with a database (e.g., a central database, column 9, lines 8-25, column 10, lines 3-5), said module to monitor the flow of at least a first image at a first network location (see figures 6-7), the first image comprising at least a first digital watermark including a first identifier (column 7, lines 3-33; column 9, lines 5-67; column 10, lines 1-10), said module comprising:

Means for determining a security level associated with the first image (digital signature and secrete keys embedded into the image, column 9, lines 8-60; column 10, lines 1-10);

Means for comparing a first image security level with a user security level (e.g., computing the signature of the original data and compare against the signature sent with the data to see if there is a match, column 6, lines 50-56; by the image authentication module 15, column 6, lines 50-56, column 9, lines 5-67, column 10, lines 1-10); and means for allowing access to the first image based on a result of said comparison step (e.g., column 6, lines 50-56, column 9, lines 8-67; column 10, lines 1-10).

Claim 29:

The claim 29 encompasses the same scope of invention as that of claim 28 except additional claimed limitation of a fragile watermark. However, Glass further discloses the claimed limitation of a fragile watermark (column 7, lines 50-55).

Remarks

9. Applicant's arguments, filed 08/01/2003, paper number 6, have been fully considered but they are not deemed to be persuasive.

10. Applicant argues in essence with respect to claim 9 and similar claims that:

"The Office cites Levy at Col. 15, lines 55-62 as teaching associating a second image in a database with a first identifier as recited in claim 9. Yet we understand the cited Levy passage to deal with a transmarking process, which, e.g., may leave an existing embedded identifier in tact and layer an additional identifier onto a media object. The transmarking process may alternatively include, e.g., adding an additional or new identifier tag to headers or footer in a file format. Respectfully, this passage is not understood to teach

associating a second image in a database with a first identifier, in combination with the remaining features of claim 9."

This is not found persuasive because Levy teaches a trans-marking process which may be performed at various stages of a media object's distribution path. For example, the identifier may be trans-marked into a watermark or other metadata format that is robust for broadcast applications and an additional identifier may be added onto a media object while leaving the existing identifier intact. In addition, Levy teaches linking an identifier to actions such as those listed in column 13, lines 50-67. Levy further teaches the identifier enables dynamic linking and the metadata or actions associated with that identifier can be changed. To change the associated metadata, the mapping process edits the identifier database to associate new metadata or actions with an identifier. Therefore, Levy teaches associating a second image (i.e., a media object) with a first identifier (i.e., the existing identifier) because the mapping process can be automated to change metadata or actions associated with an identifier at periodic intervals or in response to system events and a user may change the associated metadata or actions interactively at anytime. Furthermore, Levy teaches a web-based interface that is added to the database to facilitate access to the database (column 13, lines 29-67).

11. Applicant argues in essence with respect to claim 15 and similar claims that:

"While Glass may try to regulate access to a bank account based on evaluating a biometric image, Glass is not understood to teach or suggest: comparing a first image security level with a user security level; and allowing access to the first image based on a result of the comparison step, in combination with the remaining features of claim 15."

This is not found persuasive because Glass teaches that a gatekeeper (i.e., the authentication server, see column 8, lines 55-60) regulates access between the first user terminal (i.e., a client server) and the second user terminal (i.e., another secured resource system connected to the authentication server or an authentication server that provide a secured resource; see figures 6 and 7). Glass teaches comparing (column 9, lines 40-50) a first image security level (i.e., the digital signature, secrete key and biometric information, column 9, lines 25-60) with a user security level (e.g., the server's copy of the secret key; column 6, lines 10-40) and allowing access to the first image (i.e., the original image data embedded with a digital watermark with the digital signature, secrete key and biometric information) based on a result of the comparison step (access being allowed by the gatekeeper to a secured resource system). Glass further teaches providing the client access to the secured resource and the original secured image data original sent by the client (column 9, lines 50-60). Therefore, Glass teaches allowing access to the first image (by a client computer and/or a banking system) based on a result of the comparison step that is performed by an authentication server. Therefore, Glass fulfills the claim 15 and similar claims (claim 23, claim 28) as currently drafted.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jin-Cheng Wang whose telephone number is (703) 605-1213. The examiner can normally be reached on 8:00 AM - 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Mike Razavi can be reached on (703) 305-4713. The fax phone numbers for the organization where this application or proceeding is assigned are (703) 308-6606 for regular communications and (703) 308-6606 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 395-3900.

jcw
August 13, 2003

MICHAEL RAZAVI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600